日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００１年　１月１９日

出願番号
Application Number: 特願２００１－０１１２４８

出願人
Applicant(s): 松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年１１月３０日

特許庁長官
Commissioner,
Japan Patent Office

及川耕造

出証番号　出証特２００１－３１０５３０５

【書類名】　特許願

【整理番号】　2037320014

【提出日】　平成13年 1月19日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　3/14

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　秦　秀彦

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　稲見　聡

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　和田　浩美

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　水山　正重

【発明者】

【住所又は居所】　神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内

【氏名】　加藤　淳展

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【書類名】　明細書

【発明の名称】　情報端末装置

【特許請求の範囲】

【請求項１】サーバ装置から取得した指示データによって端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの妥当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末用データを格納する端末内データ格納手段とを備え、前記動作制御手段により前記送受信手段へ前記端末用データを取得する指示を行い、取得した前記端末用データを前記動作制御手段によって、前記端末内データ格納手段へ反映することを特徴とする情報端末装置。

【請求項２】前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記サーバ装置より取得した前記端末用データを端末の表示画面に表示させることを特徴とする請求項１記載の情報端末装置。

【請求項３】前記解析手段は、前記妥当性判定手段の結果をもとに、解析を行うことを特徴とする請求項１記載の情報端末装置。

【請求項４】前記端末用データは、端末を制御するためのデータであり、端末内データ格納手段に端末用データを反映させることにより、端末の制御を行うことを特徴とする請求項１記載の情報端末装置。

【請求項５】前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする請求項１記載の情報端末装置。

【請求項６】前記動作制御手段は、ＪＡＶＡ　ＶＭ上で動作するＪＡＶＡアプレットによって構成され、前記ＪＡＶＡアプレットはインターネット上のサーバ装置より取得することを可能とすることを特徴とする請求項１記載の情報端末装

置。

【請求項７】前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする請求項１記載の情報端末装置。

【請求項８】前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする請求項１記載の情報端末装置。

【請求項９】サーバ装置から取得した指示データによって端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの妥当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末内データを格納する端末内データ格納手段とを備え、前記解析手段の結果を、前記動作制御手段によって、端末の制御を行う前記端末内データ格納手段に反映させることを特徴とする情報端末装置。

【請求項１０】前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記動作制御手段が反映させた前記端末内データ格納手段のデータを端末の表示画面に表示させることを特徴とする請請求項９記載の情報端末装置。

【請求項１１】前記解析手段は、前記妥当性判定手段の結果をもとに、解析を行うことを特徴とする請求項９記載の情報端末装置。

【請求項１２】前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする請求項９記載の情報端末装置。

【請求項１３】前記動作制御手段は、ＪＡＶＡ　ＶＭ上で動作するＪＡＶＡアプレットによって構成され、前記ＪＡＶＡアプレットはインターネット上のサー

バ装置より取得することを可能とすることを特徴とする請求項９記載の情報端末装置。

【請求項１４】前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする請求項９記載の情報端末装置。

【請求項１５】前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする請求項９記載の情報端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報端末装置に関し、特に指示データの妥当性を判定する方式を用いることによって、周辺機器への制御を安全に行える情報端末装置に関する。

【０００２】

【従来の技術】

ＪＡＶＡのプログラム形態の一つであるＪＡＶＡアプレットにおいては、ネットワーク上で利用されることを目的としており、Ｉｎｔｅｒｎｅｔ Ｅｘｐｌｏｒｅｒ やＮｅｔｓｃａｐｅ Ｃｏｍｍｕｎｉｃａｔｏｒと言ったＷＥＢブラウザよりネットワーク側からダウンロードして実行することを可能にしている。しかし、安全面のことを考えそのようにして取得したＪＡＶＡアプレットには、周辺機器のアクセスやＩ／Ｏポートへの読み書きと言った実行に制限がかかっている。そのため、ＪＡＶＡアプレットが端末の中にあるデータの読み書きやＩ／Ｏポートへの読み書きと言った動作を行うことができなかった。

また、従来技術では、周辺機器への読み書きを行うために、ＪＡＶＡアプレットが使用するライブラリに周辺機器のドライバを組み込むことによって、解決していた（特開２０００－１１２８６４）。

【０００３】

【発明が解決しようとする課題】

しかしながら、上述のように、携帯電話や携帯情報端末など、自由にＪＡＶＡＶＭに含まれるＪＡＶＡライブラリを、追加できない装置にあとからライブラリを追加することは不可能である。

【０００４】

このような装置にライブラリを追加するためには、あらかじめ、商品出荷時にこのようなライブラリを組み込んでおく必要がある。しかし、このようにしてしまうと、全てのユーザが周辺機器へアクセスできるライブラリを使用できてしまうことになってしまう。

【０００５】

また、携帯電話といった端末に関しては、利用者個人の特別な情報（電話番号、住所録など）が格納されている。このような情報を特権のないユーザが引き出せてしまうことは問題である。

【０００６】

本発明は、上記従来技術の問題を解決し、周辺機器へアクセスするプログラムには、特権を持たせることによって、安全に周辺機器へのアクセスを行えることを特徴とする情報端末装置を提供することを目的とする。

【０００７】

【課題を解決するための手段】

上記課題を解決するために、サーバ装置から取得した指示データによって端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの妥当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末用データを格納する端末内データ格納手段とを備え、前記動作制御手段により前記送受信手段へ前記端末用データを取得する指示を行い、取得した前記端末用データを前記動作制御手段によって、前記端末内データ格納手段へ反映することを特徴とする。

【０００８】

更に、前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記サーバ装置より取得した前記端末用データを端末の表示画面に表示させることを特徴とする。

【０００９】

また、前記解析手段と、前記妥当性判定手段は、前記妥当性判定手段の結果をもとに、前記解析手段を行うことを特徴とする。

【００１０】

また、前記端末用データは、端末を制御するためのデータであり、端末内データ格納手段に端末用データを反映させることにより、端末の制御を行うことを特徴とする。

【００１１】

また、前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする。

【００１２】

また、前記動作制御手段は、ＪＡＶＡ　ＶＭ上で動作するＪＡＶＡアプレットによって構成され、前記ＪＡＶＡアプレットはインターネット上のサーバ装置より取得することを可能とすることを特徴とする。

【００１３】

また、前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする。

【００１４】

また、前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする。

【００１５】

更に、上記課題を解決するために、サーバ装置から取得した指示データによっ

て端末を制御する情報端末装置において、前記サーバ装置から前記指示データを取得する送受信手段と、前記送受信手段によって取得した指示データを格納する受信データ格納手段と、前記受信データ格納手段に格納した前記指示データを参照し、解析を行う解析手段と、前記解析手段により、解析した結果より指示データの当性を判定する妥当性判定手段と、前記妥当性判定手段より前記指示データが妥当であると判定された際は、前記指示データの内容に従い動作を行う動作制御手段と、端末内データを格納する端末内データ格納手段とを備え、前記解析手段の結果を、前記動作制御手段によって、端末の制御を行う前記端末内データ格納手段に反映させることを特徴とする。

【００１６】

更に、前記端末内データ格納手段に格納した前記端末用データを端末の表示画面に表示させる表示手段を備え、前記動作制御手段が反映させた前記端末内データ格納手段のデータを端末の表示画面に表示させることを特徴とする。

【００１７】

また、前記解析手段と、前記妥当性判定手段は、前記妥当性判定手段の結果をもとに、前記解析手段を行うことを特徴とする。

【００１８】

また、前記指示データは、暗号化が行われており、前記解析手段は、暗号化された前記指示データを復号することを特徴とする。

【００１９】

また、前記動作制御手段は、ＪＡＶＡ　ＶＭ上で動作するＪＡＶＡアプレットによって構成され、前記ＪＡＶＡアプレットはインターネット上のサーバ装置より取得することを可能とすることを特徴とする。

【００２０】

また、前記動作制御手段は、前記送受信手段によって取得した前記端末用データを前記端末内データ格納手段に格納する前に妥当性の判定を行い、前記端末内データが妥当であることが判定された際に、前記指示データの内容に従って処理を行うことを特徴とする。

【００２１】

また、前記端末内データ格納手段は、端末内に存在するデータ出力手段であり、前記解析手段の結果を、前記動作制御手段によって、前記データ出力手段に出力することを特徴とする。

【００２２】

【発明の実施の形態】

以下、本発明の実施例を図面を用いて詳細に説明する。

【００２３】

（実施の形態１）

図１は、本発明の実施の形態１の情報端末装置を示すブロック図である。図１において、サーバ装置１０１は、インターネット上に存在し、ＨＴＭＬ、画像データを保持し、要求に応じて、これらのデータを要求元へ送出する装置である。指示データ１０２は、サーバ装置１０１上に存在し、情報端末装置１０４への指示が記述されている。また、端末用データ１０３は、指示データ１０２によって、情報端末装置１０４が取得する端末用のデータである。情報端末装置１０４は、インターネット上のデータを取得し、表示することができる装置である。データ取得要求手段１０５は、指示データ１０２を取得するための手段である。送受信手段１０６は、データ取得要求手段１０５より要求のあったＵＲＬのデータを取得するための手段である。受信データ格納手段１０７は、送受信手段によって取得したデータを格納する手段である。解析手段１０８は、受信データ格納手段１０７に格納されている指示データを解析するための手段である。解析結果格納手段１０９は、解析手段１０８によって解析したデータを格納するための手段である。妥当性判定手段１１０は、解析結果格納手段１０９に格納されているデータより、指示データ１０２が妥当なデータであることを判定するための手段である。動作制御手段１１１は、妥当性判定手段１１０によって、指示データ１０２が妥当であると判定された際に、指示データ１０２に基づいて動作を行う手段である。端末内データ格納手段１１２は、動作制御手段１１１から送受信手段１０６へ取得要求を出し、その結果取得し、受信データ格納手段１０７に格納した端末用データ１０３を格納する手段である。表示手段１１３は、端末内データ格納手段１１２によって格納されている端末用データを用いて、表示を行うための手

段である。データ出力手段１１４は、動作制御手段１１１によって、指示されたデータを出力するための手段である。

【００２４】

上記のように構成された実施の形態１の情報端末装置の動作について、図２のフローチャートを用いて説明する。データ取得処理（ステップ２０１）では、情報端末装置１０４は、ＷＥＢブラウザに表示している画面からアンカーを選択するなどして、指示データ１０２を取得要求を行う処理を行う。送受信処理（ステップ２０２）では、データ取得処理（ステップ２０１）より取得要求のあった指示データ１０２を取得する処理を行う。解析処理（ステップ２０３）では、取得した指示データ１０２の解析を行う。妥当性判定処理（ステップ２０４）では、解析処理（ステップ２０３）の結果をもとに取得した指示データ１０２が妥当なデータであるかどうかを判定する。動作制御処理（ステップ２０５）では、指示データに記述された内容に従って端末用データ１０３を取得する処理を行う。送受信処理（ステップ２０６）では、指示データに端末用データを取得する内容が記述されている際は、データの取得を行う。複数の端末用データの取得が記述されている際は、複数回データの取得を行う。表示処理（ステップ２０７）では、動作制御処理（ステップ２０５）と送受信処理（ステップ２０６）によって取得した端末用データの表示を行う。

【００２５】

ステップ２０２において送受信手段１０６によってサーバ装置１０１から取得できるデータについて図６、図８を用いて説明する。サーバ装置１０１より取得する指示データは、図６のようにＸＭＬ（Ｅｘｔｅｎｄｅｄ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）形式のフォーマットを持つ。なお、このフォーマットは「タグ名：値」と言った形式でもよく、このフォーマットのみに限らない。ｐｒｏｔｅｃｔｅｄタグ６０１とｄａｔａＳｏｕｒｃｅＵｒｌタグ６０２とｓｉｇｎａｔｕｒｅタグ６０４、ｃｅｒｔｉｆｉｃａｔｅタグ６０５が妥当性の判定に用いられる部分である。ｐｒｏｔｅｃｔｅｄタグ６０１の部分に端末装置１０４に対する指示内容が記述される。端末用データ１０３として取得されるデータが、図８である。ｄａｔａＳｏｕｒｃｅＵｒｌタグ６０２の部分に記述されている内容がに

わとりの画像データ８０１、パンダの画像データ８０２と言ったデータである。なお、このデータは画像データのみではなく、音楽データや制御用データであっても構わない。また、ｅｘＤａｔａＤｉｇｅｓｔタグ６０３は、ステップ２０５で端末用データ１０３の妥当性の判定に用いられる。指示データ１０２は、ステップ２０３で受信した際は、ＤＥＳアルゴリズムによって暗号化が行われている。なお、この暗号化に用いられる方式は、ＤＥＳアルゴリズムに関わらず、様々な暗号化方式で暗号化される。

【００２６】

次にステップ２０３について図３を用いて説明する。暗号復号処理（ステップ３０２）では、指示データ１０２が暗号化されている際は、暗号化されている指示データ１０２の復号化を行う。また、復号化のアルゴリズムには、ＤＥＳなどの様々なアルゴリズムが用いられる。なお、指示データ１０２は、必ずしも復号されているとは限らない。指示データ解析処理（ステップ３０３）では、復号化が終了した指示データの解析を行う。解析の結果は、解析結果格納手段１０９に格納される。

【００２７】

図７はステップ２０３によって、解析された結果が解析結果格納手段１０９に格納される一例を示している。解析に用いた指示データの種類を識別するための情報（ｄｅｓｃｒｉｐｔｏｒＴｙｐｅ）には、Ｃｕｓｔｏｍｉｓｅが格納されている。指示データのバージョンを示す情報（ＦＩＤ）には、１が格納されている。指示データを受けて動作制御部が取得しに行く必要がある端末用データ１０３が格納されている場所（ｄａｔａＳｏｕｒｃｅＵｒｌ）には、ｈｔｔｐｓ：／／ｗｗｗ．ｈｏｇｅ．ｃｏｍ／ｆｏｏ１．ｇｉｆとｈｔｔｐｓ：／／ｗｗｗ．ｈｏｇｅ．ｃｏｍ／ｆｏｏ２．ｇｉｆが格納されている。ｄａｔａＳｏｕｒｃｅＵｒｌが示す端末用データを、ＭＤ５アルゴリズムを用いてハッシュ化した情報（ｅｘＤａｔａＤｉｇｉｔ）にはそれぞれに対応してａｆｄｆｓａｆａｆａｆｋｌｊｋ：ｊｂａｈａｆｌｋｄｊｆａとｂｈｏｕｙｂｙｏｕｈｓｄｈｏｌｉｄｉｏｕｙｂｓが格納されている。署名の情報（ｓｉｇｎａｔｕｒｅ）には署名が格納されている。署名者の証明書を格納する情報（ｃｅｒｔｉｆｉｃａｔｅ）には、その

値である署名者の証明書と二次ＣＡの証明書が格納される。なお、場合によっては、二次ＣＡ証明書は存在しない場合もあり、更に三次、四次と続く場合もある。

【００２８】

次にステップ２０４について図４と図６を用いて説明する。指示データ６０６の＜ｐｒｏｔｅｃｔｅｄ＞タグと＜／ｐｒｏｔｅｃｔｅｄ＞タグ囲まれるデータについてＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　５）アルゴリズムでハッシュ化を行う（ステップ４０２）。なお、ハッシュ化を行うためのアルゴリズムは、ＭＤ５だけに限らない。なお、ハッシュ化を行う指示データの範囲は、指示データ６０６に限るものではなく、取り決めることができる。Ｎ次証明書の妥当性判定処理（ステップ４０３）と署名者の証明書の判定処理（ステップ４０４）では、ｃｅｒｔｉｆｉｃａｔｅタグ６０５の署名者の証明書が妥当であると証明できるまで、順に証明書、二次証明書と利用し、場合によっては、Ｎ次証明書を利用して妥当性の判定を行う。なお、証明書はインターネットの世界で一般的に用いられている公開鍵暗号方式に用いられる証明書である。公開鍵取得処理（ステップ４０５）では、署名者の証明書より公開鍵の取得を行う。署名復号化処理（ステップ４０６）では、署名部分６０４を公開鍵取得処理で取得した公開鍵を用いることによって復号を行う。ハッシュ化データ比較処理（ステップ４０７）では、ステップ４０２で取得したハッシュ値とステップ４０６で取得した署名の値を比較する。比較結果が正しければ指示データ６０６は妥当だと証明されたデータと考えられる。なお、ステップ４０３に、用いられる妥当性を判定する処理には、公開鍵暗号方式だけに限らない。

【００２９】

次に図５を用いてステップ２０５の説明をする。まず解析結果格納手段１０９を参照し、データ取得判定処理（ステップ５０２）を行う。解析結果格納手段１０９に取得すべき端末内データが存在するだけデータ取得処理（ステップ５０３）に取得を行う。データ妥当性判定処理（ステップ５０４）では、取得した端末用データ１０３が妥当であるか否かの判定を行う。妥当性の判定は、取得したデータをＭＤ５アルゴリズムでハッシュ化し、その値が解析結果格納手段１０９に

格納されているＭＤ５の値と比較し、等しければ妥当だと判定する。なお、ステップ５０４はなくても構わない。なお、ステップ５０４に用いるアルゴリズムはＭＤ５アルゴリズムに限らない。端末内データ格納処理（ステップ５０５）では、妥当性を判定できた端末用データ１０３を端末内のデータとして格納する。なお、ステップ２０５は、ＪＡＶＡアプレットのように動的に端末にダウンロードされるプログラムであっても構わない。なお、指示データに内容によって取得した端末用データを端末内データ格納手段１１２に格納するのではなく、データ出力手段（周辺機器、ＩｒＤＡなど）に出力することも考えられる。

【００３０】

図２に示されるステップを行った結果、表示処理（ステップ２０７）で表示される様子を図９に示す。本発明によって表示が変更される前の様子９０１が、本発明によって表示が変更された後の様子９０２になる。本発明によって、端末内のデータの変更を安全に行い、表示する様子を変更することができた。

【００３１】

（実施の形態２）

図１は、本発明の実施の形態２の情報端末装置を示すブロック図であり、実施の形態１の構成と同じである。情報端末装置の動作について、図１０のシーケンス図を用いて説明する。データ取得処理（ステップ２０１）では、情報端末装置１０４は、ＷＥＢブラウザに表示している画面からアンカーを選択するなどして、指示データ１０２を取得要求を行う処理を行う。送受信処理（ステップ２０２）では、データ取得処理（ステップ２０１）より取得要求のあった指示データ１０２を取得する処理を行う。解析処理（ステップ２０３）では、取得した指示データ１０２の解析を行う。妥当性判定処理（ステップ２０４）では、解析処理（ステップ２０３）の結果をもとに取得した指示データ１０２が妥当なデータであるかどうかを判定する。動作制御処理（ステップ１００５）では、指示データに記述された内容に従って端末内のデータを変更する処理を行う。複数の端末用データの変更が記述されている際は、複数回データの変更を行う。端末内データ格納処理（ステップ１００６）では、動作制御処理（ステップ１００５）によって指定されたデータの変更を行う。

【００３２】

ステップ２０２によってサーバ装置１０１から取得できるデータについて図１１を用いて説明する。サーバ装置より取得する指示データは、図１１のようにＸＭＬ（Ｅｘｔｅｎｄｅｄ　Ｍａｒｋｕｐ　Ｌａｎｇｕａｇｅ）形式のフォーマットを持つ。なお、このフォーマットは「タグ名：値」と言った形式でもよく、このフォーマットのみに限らない。ｐｒｏｔｅｃｔｅｄタグ１１０１とｓｉｇｎａｔｕｒｅタグ１１０３、ｃｅｒｔｉｆｉｃａｔｅタグ１１０４が妥当性の判定に用いられる部分である。ｐｒｏｔｅｃｔｅｄタグ１１０１の部分に端末装置１０４に対する指示内容が記述される。指示データ１０２は、ステップ２０３で受信した際は、ＤＥＳアルゴリズムによって暗号化が行われている。なお、この暗号化に用いられる方式は、ＤＥＳアルゴリズムに関わらず、様々な暗号化方式で暗号化される。

【００３３】

ステップ２０３については実施の形態１と同様であるので省略する。

【００３４】

図１２はステップ２０３によって、解析された結果が解析結果格納手段１０９に格納される一例を示している。解析に用いた指示データの種類を識別するための情報（ｄｅｓｃｒｉｐｔｏｒＴｙｐｅ）には、Ｃｏｎｔｒｏｌが格納されている。指示データのバージョンを示す情報（ＦＩＤ）には、１が格納されている。指示データを受けて動作制御部がデータを反映する情報が格納されている場所（ｃｔｒｌＤａｔａ）には、１２３が格納されている。署名の情報（ｓｉｇｎａｔｕｒｅ）には署名が格納されている。証明書を格納する情報（ｃｅｒｔｉｆｉｃａｔｅ）には、その値である署名者の証明書と二次ＣＡの証明書が格納されている。なお、場合によっては、二次ＣＡ証明書は存在しない場合もあり、更に三次、四次と続く場合もある。

【００３５】

次にステップ２０４について図４と図１１を用いて説明する。指示データ１１０５の＜ｐｒｏｔｅｃｔｅｄ＞タグと＜／ｐｒｏｔｅｃｔｅｄ＞タグ囲まれるデータについてＭＤ５（Ｍｅｓｓａｇｅ　Ｄｉｇｅｓｔ　５）アルゴリズムでハッ

シュ化を行う（ステップ４０２）。なお、ハッシュ化を行うためのアルゴリズムは、ＭＤ５だけに限らない。なお、ハッシュ化を行う指示データの範囲は、指示データ１１０１の部分に限るものではなく、取り決めることができる。Ｎ次証明書の妥当性判定処理（ステップ４０３）と署名者の証明書の判定処理（ステップ４０４）では、ｃｅｒｔｉｆｉｃａｔｅタグ１１０４の署名者の証明書が妥当であると証明できるまで、順に証明書、二次証明書と利用し、場合によっては、Ｎ次証明書を利用して妥当性の判定を行う。なお、証明書はインターネットの世界で一般的に用いられている公開鍵暗号方式に用いられる証明書である。公開鍵取得処理（ステップ４０５）では、署名者の証明書より公開鍵の取得を行う。署名復号化処理（ステップ４０６）では、署名部分１１０３を公開鍵取得処理で取得した公開鍵を用いることによって復号を行う。ハッシュ化データ比較処理（ステップ４０７）では、ステップ４０２で取得したハッシュ値と署名復号化処理（ステップ４０６）で取得した署名の値を比較する。比較結果が正しければ指示データ１１０５は妥当性だと証明されたデータと考えられる。なお、妥当性判定処理に、用いられる妥当性を判定する処理には、公開鍵暗号方式だけに限らない。

【００３６】

次に図１３を用いてステップ１００５の説明をする。まず解析結果格納手段１０９を参照し、データ取得判定処理（ステップ１３０２）を行う。解析結果格納手段１０９に取得すべき端末内データが存在するだけデータ取得処理（ステップ１３０３）にて取得を行う。端末内データ格納処理（ステップ１３０５）では、指示データに記述されたデータを端末内のデータとして端末内データ格納手段１１２に格納する。なお、ステップ１３０５は、ＪＡＶＡアプレットのように動的に端末にダウンロードされるプログラムであっても構わない。なお、指示データに記述された内容を端末内データ格納手段１１２に格納するのではなく、データ出力手段１１４（周辺機器、ＩｒＤＡなど）に出力することも考えられる。

【００３７】

図１０に示されるステップを行った結果、端末内のデータを変更することができた。

【００３８】

【発明の効果】

ＪＡＶＡアプレットのみに限らず、周辺機器へアクセスするプログラムにおいて、指示データに自身の妥当性を判定する方式を用いることによって、周辺機器の制御を安全に行える。

【図面の簡単な説明】

【図１】

本発明の実施の形態の情報端末装置の示す全体構成図

【図２】

本発明の実施の形態１の情報端末装置の動作を示すフローチャート

【図３】

本発明の実施の形態１の解析処理を示すフローチャート

【図４】

本発明の実施の形態１の妥当性判定処理を示すフローチャート

【図５】

本発明の実施の形態１の動作制御処理を示すのフローチャート

【図６】

本発明の実施の形態１の指示データの一例を示す図

【図７】

本発明の実施の形態１の指示データの解析結果の一例を示す図

【図８】

本発明の実施の形態１の端末用データの一例を示す図

【図９】

本発明の実施の形態１の動作結果の一例を示す図

【図１０】

本発明の実施の形態２の情報端末装置の動作を示すフローチャート

【図１１】

本発明の実施の形態２の指示データの一例を示す図

【図１２】

本発明の実施の形態２の指示データの解析結果の一例を示す図

【図１３】

本発明の実施の形態２の動作制御処理を示すフローチャート

【符号の説明】

１０１　サーバ装置

１０２　指示データ

１０３　端末用データ

１０４　情報端末装置

１０５　データ取得要求手段

１０６　送受信手段

１０７　受信データ格納手段

１０８　解析手段

１０９　解析結果格納手段

１１０　妥当性判定手段

１１１　動作制御手段

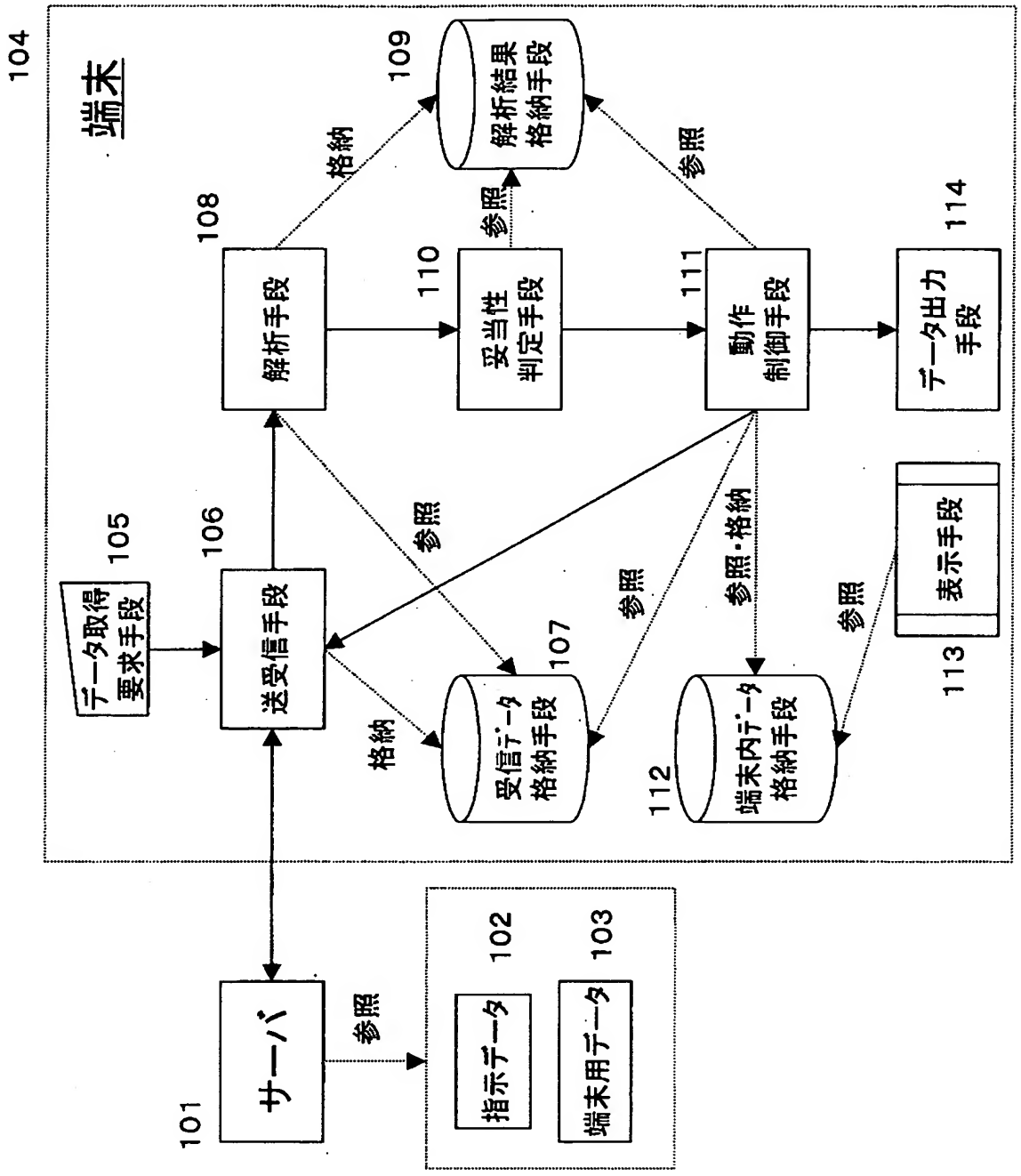
１１２　端末内データ格納手段

１１３　表示手段

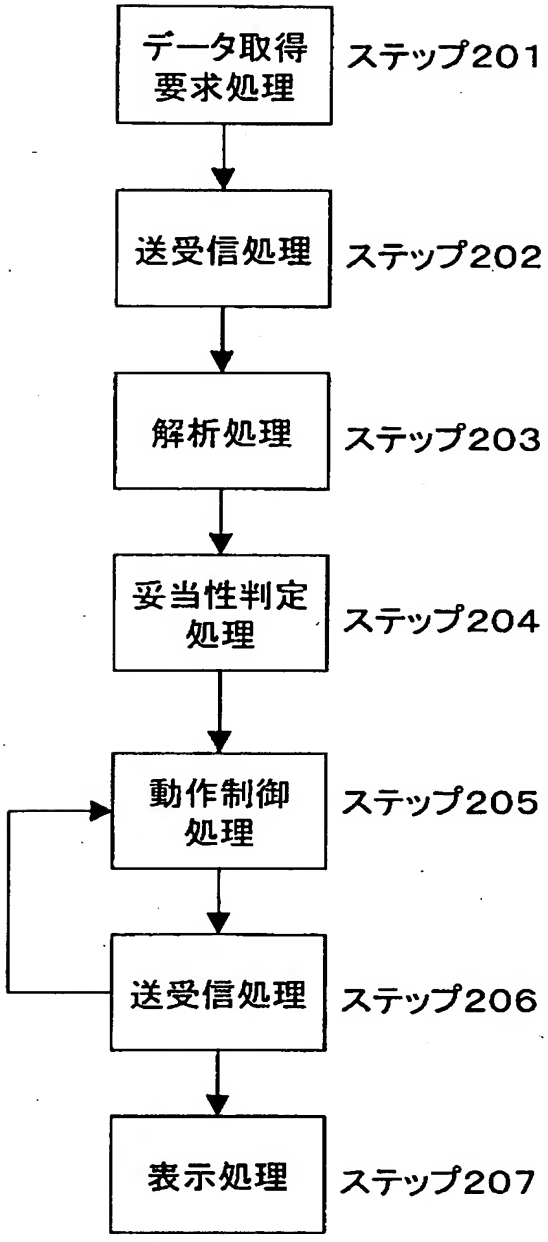
１１４　データ出力手段

【書類名】　　図面

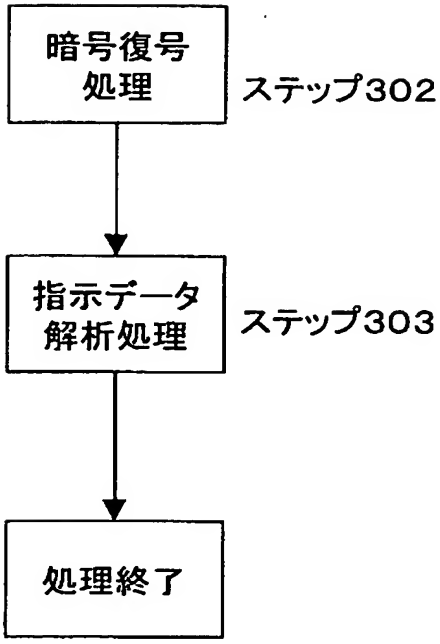
【図１】


104
端末
109
解析結果格納手段
格納
参照
108
解析手段
110
妥当性判定手段
111
動作制御手段
114
データ出力手段
105
データ取得要求手段
106
送受信手段
107
受信データ格納手段
112
端末内データ格納手段
113
表示手段
参照・格納
101
サーバ
102
指示データ
103
端末用データ

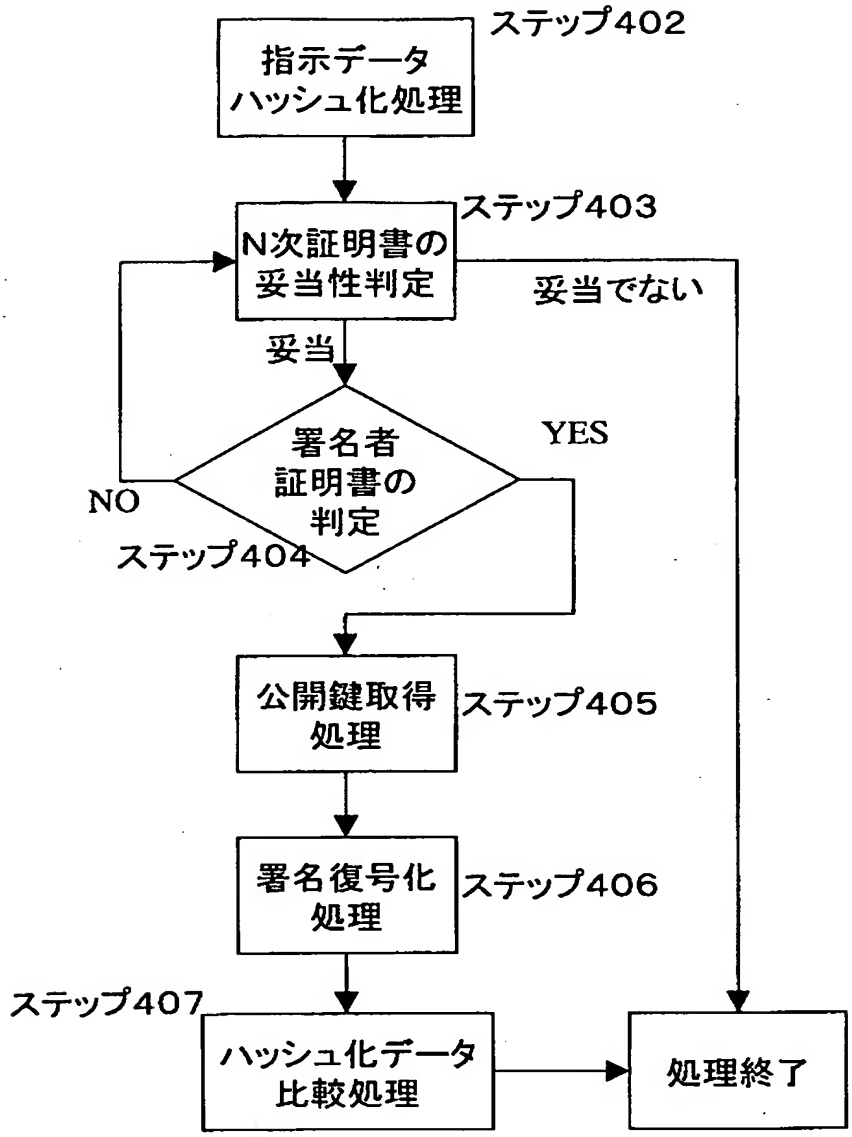
【図２】


データ取得要求処理
ステップ201
送受信処理
ステップ202
解析処理
ステップ203
妥当性判定処理
ステップ204
動作制御処理
ステップ205
送受信処理
ステップ206
表示処理
ステップ207

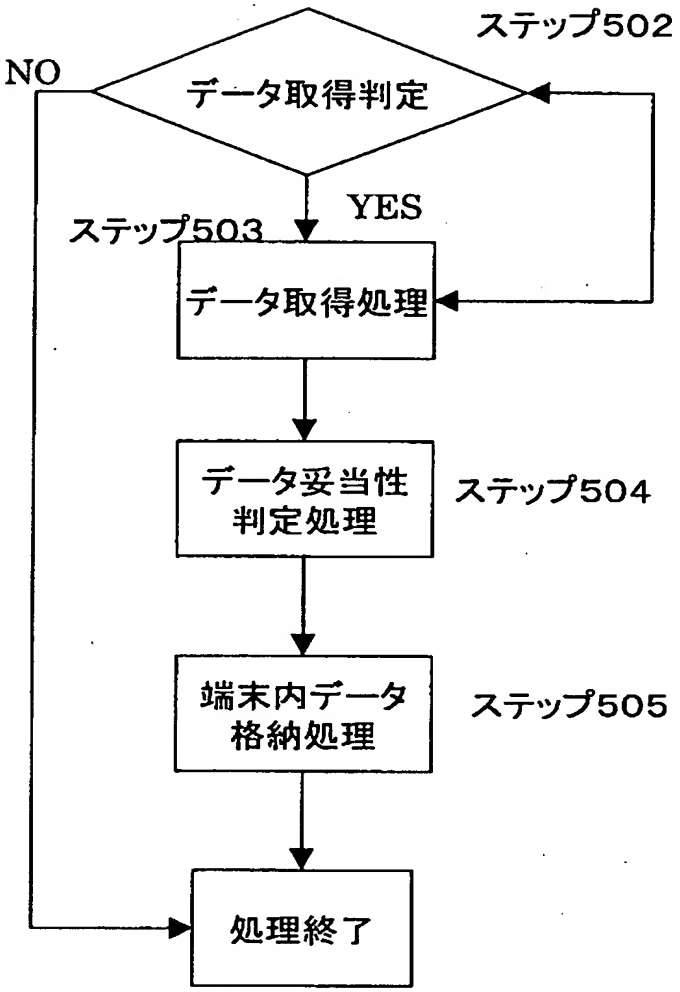
【図３】



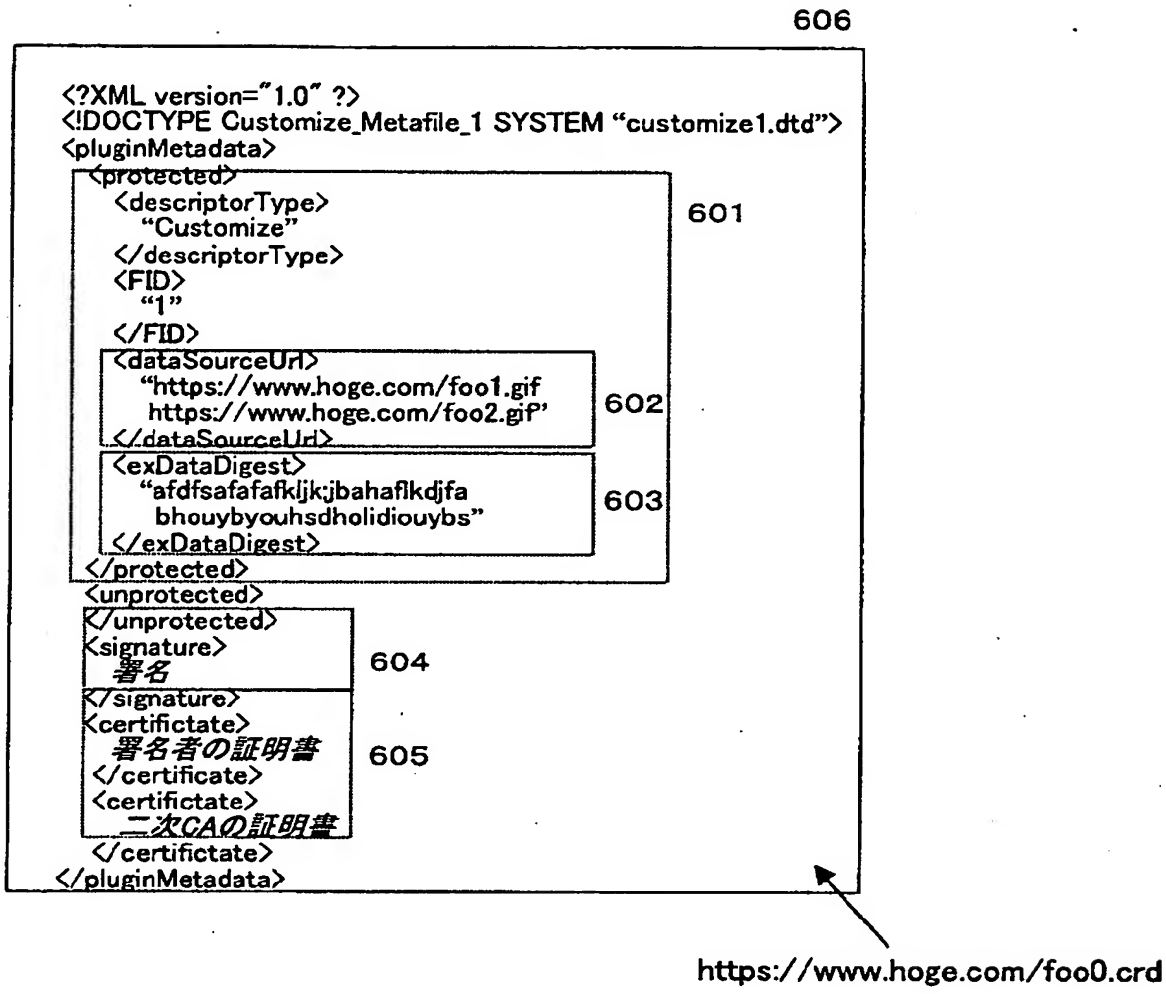
【図４】


ステップ402
指示データ
ハッシュ化処理
ステップ403
N次証明書の
妥当性判定
妥当でない
妥当
署名者
証明書の
判定
YES
NO
ステップ404
公開鍵取得
処理
ステップ405
署名復号化
処理
ステップ406
ステップ407
ハッシュ化データ
比較処理
処理終了

【図５】


ステップ502
NO
データ取得判定
YES
ステップ503
データ取得処理
データ妥当性
判定処理
ステップ504
端末内データ
格納処理
ステップ505
処理終了

【図６】


606
<?XML version="1.0" ?>
<!DOCTYPE Customize_Metafile_1 SYSTEM "customize1.dtd">
<pluginMetadata>
<protected>
<descriptorType>
"Customize"
</descriptorType>
<FID>
"1"
</FID>
<dataSourceUrl>
"https://www.hoge.com/foo1.gif
https://www.hoge.com/foo2.gif"
</dataSourceUrl>
<exDataDigest>
"afdfsafafafkljk;jbahaflkdjfa
bhouybyouhsdholidiouybs"
</exDataDigest>
</protected>
<unprotected>
</unprotected>
<signature>
署名
</signature>
<certifictate>
署名者の証明書
</certificate>
<certifictate>
二次CAの証明書
</certifictate>
</pluginMetadata>
601
602
603
604
605
https://www.hoge.com/foo0.crd

【図７】

descriptorType	Customize
FID	1
dataSourceUrl	https://www.hoge.com/foo1.gif
dataSourceUrl	https://www.hoge.com/foo2.gif
exDataDigest	afdfsafafafkljk;jbahaflkdjfa
exDataDigest	bhouybyouhsdholidiouybs
signature	*署名*
certificate	*署名者の証明書*
certificate	*二次CAの証明書*

【図８】

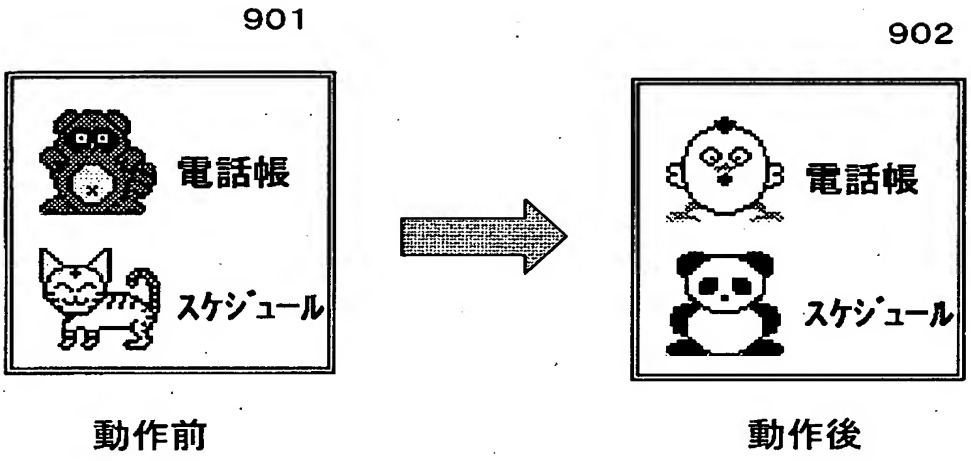
https://www.hoge.com/foo1.gif

801

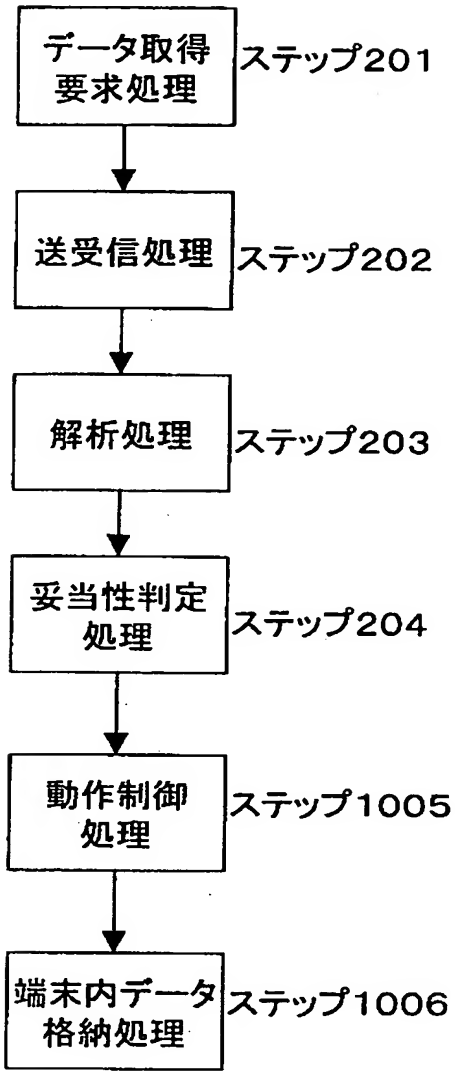
https://www.hoge.com/foo2.gif

802

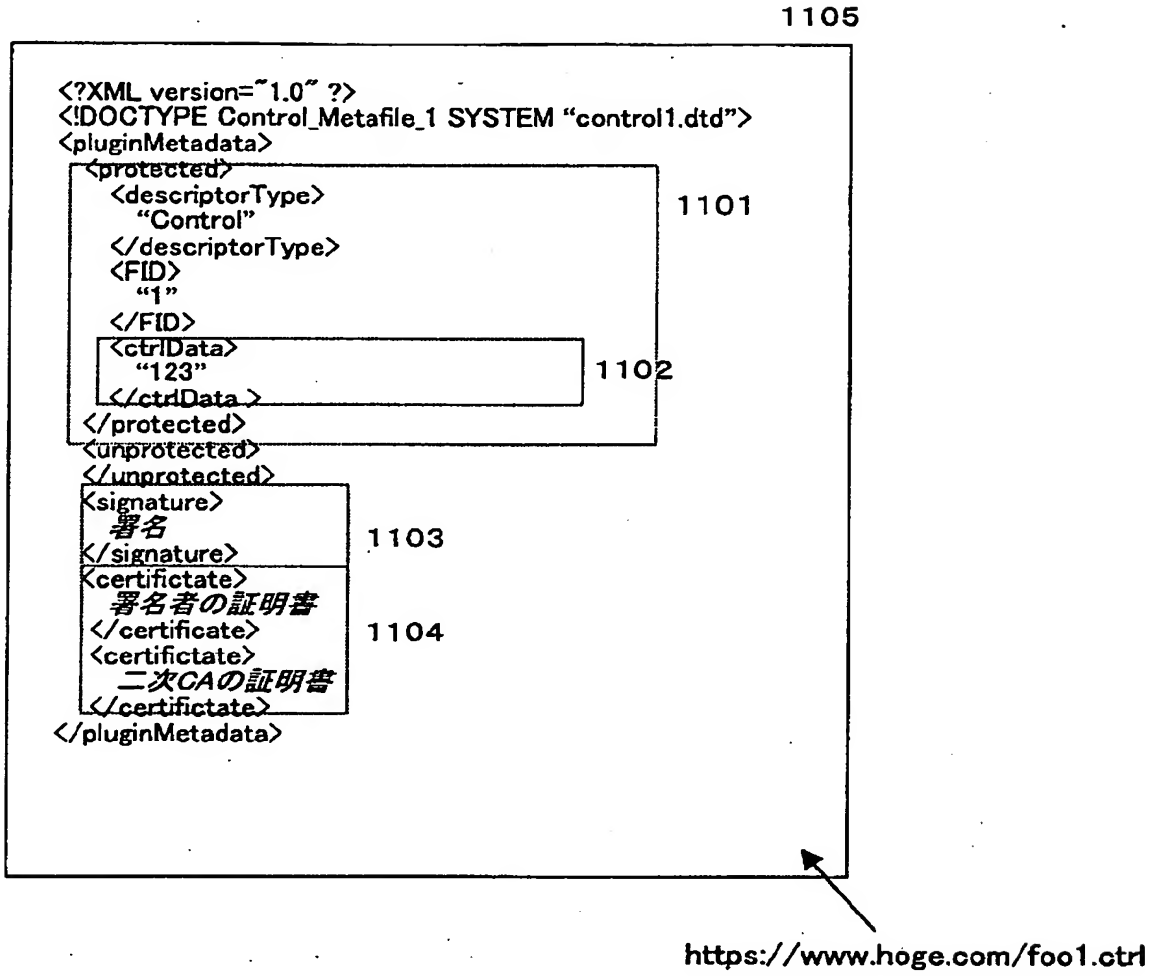
【図９】



【図１０】


データ取得要求処理
ステップ201
送受信処理
ステップ202
解析処理
ステップ203
妥当性判定処理
ステップ204
動作制御処理
ステップ1005
端末内データ格納処理
ステップ1006

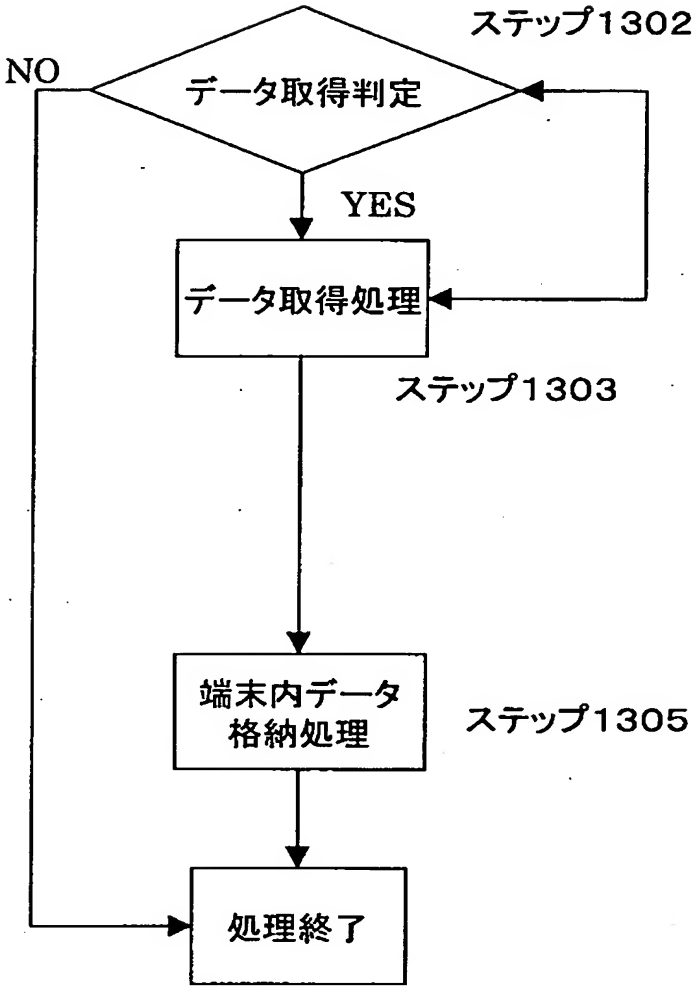
【図１１】


1105
<?XML version="1.0" ?>
<!DOCTYPE Control_Metafile_1 SYSTEM "control1.dtd">
<pluginMetadata>
<protected>
<descriptorType>
"Control"
</descriptorType>
<FID>
"1"
</FID>
<ctrlData>
"123"
</ctrlData>
1101
1102
</protected>
<unprotected>
</unprotected>
<signature>
署名
</signature>
1103
<certifictate>
署名者の証明書
</certificate>
<certifictate>
二次CAの証明書
</certifictate>
1104
</pluginMetadata>
https://www.hoge.com/foo1.ctrl

【図１２】

descriptorType	Control
FID	1
ctrlData	123
signature	*署名*
certificate	*署名者の証明書*
certificate	*二次CAの証明書*

【図１３】


ステップ1302
NO
データ取得判定
YES
データ取得処理
ステップ1303
端末内データ
格納処理
ステップ1305
処理終了

【書類名】　要約書

【要約】

【課題】　安全面を考慮するとＪＡＶＡアプレットといったプログラムから端末の周辺機器を制御することができなかった。

【解決手段】　ＪＡＶＡアプレットのみに限らず、周辺機器へアクセスするプログラムにおいて、指示データに自身の妥当性を判定する方式を用いることによって、周辺機器の制御を安全に行える。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社